UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/635,778	08/11/2000	David M. Goldschlag	2685/5681	1089

7590 03/31/2006

WENDY E. KOBA, ESQ
P.O. BOX 556
SPRINGTOWN,, PA 18081-0556

EXAMINER	
VAN BRAMER, JOHN W	
ART UNIT	**PAPER NUMBER**
3622	

DATE MAILED: 03/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/635,778	GOLDSCHLAG ET AL.	
	Examiner	Art Unit	
	John Van Bramer	3622	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *13-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The amendment filed on January 30, 2006 added no claims, cancelled no claims, and amended no claims. The currently pending claims considered below are Claims 13-27.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 13-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Challener et al (6,081,793).

Claims 13, 15, 17, 21-24: Challener discloses a system, apparatus, and program for electronic voting, comprising:

a. A processor (Item 55, Figure 2b);

b. Instructions to cause the processor to perform the steps of:

1. Receiving a voter registration request message (ballot request) that will bind vote authorization data (voter identification and PIN) and a blinded unvalidated vote certificate (ballot)(col 6, line 65 – col 7, line 4);
2. Determine if the vote authorization data is valid (col 7, lines 4-16);
3. Validating the blinded unvalidated vote certificate to obtain a blinded vote certificate if the vote authorization data is valid (col 7, lines 4-16); and
4. Sending a response message to the voter that includes the blinded validated vote certificate (certified ballot) atomically bound to the voter registration request message (col 7, lines 4-16); and

c. Memory coupled to the processor (col 3, lines 30-35).

The Examiner notes that Challener discloses that the user receives a smart card when registering to vote. The smart card contains the voter identification, public encryption key, a ballot box ID, and a PIN number for the voter (i.e. vote authorization data). On election day, the voter places his smart card in a smart card reader of the authentication server at the polling station and enters his PIN number to validate his identity which generates a "ballot request". The Examiner considers the entering of the smart card information and the PIN number and the resultant ballot request to be the equivalent of the claimed voter registration request message. The authentication server uses the PIN number to determine if the smart card information (vote authorization data) is valid. If the vote authorization data is valid, the polling station selects a ballot ID, encrypts it along with the voter authorization data and "sends the encrypted ballot, and the ballot ID, to the voter's personal computer" (col 8, lines 1-9). The voter then decrypts the ballot with the smart card encryption key, enters his

selections onto the ballot, re-encrypts the ballot using the smart card encryption key, and returns the encrypted ballot to the voting system. The system uses at least two servers, each able to decrypt only a portion of the encrypted ballot to maintain the anonymity of the voter, while also allowing for the verification of the vote, if necessary. Thus, Challener uses blinded encryption methods. The Examiner considers the initial ballot selected by the polling station to be the equivalent of the claimed blinded unvalidated voter certificate; the encrypted ballot sent to the voter's personal computer as the blinded validated voter certificate.

Claims 14, 16, and 18: Challener discloses an apparatus for electronic voting as in Claims 13, 15, and 17 above, and further inherently discloses the certificate indicating a yes or no vote (col 1, lines 11-15). The Examiner notes that ballots contain one or more questions to which the voter may make one or more selections based on his desires. Each of these selections is a vote for or against the topic of the question – whether it is a "for" (yes) or "against" (no) vote on a local tax levy proposition, "for" (yes) or "against" (no) the Presidential candidates, or "for" (yes) or "against" (no) several candidates running for several open councilmen positions. In each case, the completed ballot indicates the voter's yes or no votes.

Claim 19: Challener discloses an apparatus for electronic voting, comprising:

a. A processor (Item 55, Figure 2b);

b. Instructions to cause the processor to perform the steps of:

1. Receiving a voter registration request message (ballot request) that will bind vote authorization data (voter identification and PIN) and a blinded unvalidated vote certificate (ballot)(col 6, line 65 – col 7, line 4);
2. Determine if the vote authorization data is valid (col 7, lines 4-16);
3. Validating the blinded unvalidated vote certificate to obtain a blinded vote certificate if the vote authorization data is valid (col 7, lines 4-16); and
4. Sending a response message to the voter that includes the blinded validated vote certificate (certified ballot) atomically bound to the voter registration request message (col 7, lines 4-16); and

c. Memory coupled to the processor (col 3, lines 30-35).

The Examiner notes that Challener discloses that the user receives a smart card when registering to vote. The smart card contains the voter identification, public encryption key, a ballot box ID, and a PIN number for the voter (i.e. vote authorization data). On election day, the voter places his smart card in a smart card reader of the authentication server at the polling station and enters his PIN number to validate his identity which generates a "ballot request". The Examiner considers the entering of the smart card information and the PIN number and the resultant ballot request to be the equivalent of the claimed voter registration request message. The authentication server uses the PIN number to determine if the smart card information (vote authorization data) is valid. If the vote authorization data is valid, the polling station selects a ballot ID, encrypts it along with the voter authorization data and "sends the encrypted ballot, and the ballot ID, to the voter's personal computer" (col 8, lines 1-9). The voter then decrypts the ballot with the smart card

encryption key, enters his selections onto the ballot, re-encrypts the ballot using the smart card encryption key, and returns the encrypted ballot to the voting system. The system uses at least two servers, each able to decrypt only a portion of the encrypted ballot to maintain the anonymity of the voter, while also allowing for the verification of the vote, if necessary. Thus, Challener uses blinded encryption methods. The Examiner considers the initial ballot selected by the polling station to be the equivalent of the claimed blinded unvalidated voter certificate; the encrypted ballot sent to the voter's personal computer as the blinded validated voter certificate.

Challener also discloses methods to tabulate, correct, or challenge the votes through the use of a journal server which keeps track of each vote as it is being entered. To correct a vote, the voter again enters his PIN number and smart card data (which includes the validated ballot)(i.e. "receives a second voting transaction message)", the system revalidates the voter (ballot)(i.e. "determines if the second voting transaction message has the same nonce, session key, and blinding factor" as the previous stored ballot); and retrieves the previously stored ballot if the second request message is valid (col 10, line 51 – col 11, line 37).

Claim 20: Challener discloses an apparatus for electronic voting as in Claim 19 above, and further inherently discloses the certificate indicating a yes or no vote (col 1, lines 11-15). The Examiner notes that ballots contain one or more questions to which the voter may make one or more selections based on his desires. Each of these selections is a vote for or against the topic of the question – whether it is a "for" (yes) or "against" (no) vote on a

local tax levy proposition, "for" (yes) or "against" (no) the Presidential candidates, or "for" (yes) or "against" (no) several candidates running for several open councilmen positions. In each case, the completed ballot indicates the voter's yes or no votes.

Claims 25-27: Challener discloses a system for electronic voting as in Claim 24 above, and further discloses means for auditing, initializing, and recovering from an interruption in an electronic voting transaction (col 10, line 51 – col 11, line 37).

Response to Arguments

4 Applicant's arguments filed January 30, 2006 have been fully considered but they are not persuasive. The applicant argues that the Challener et al. reference does not disclose or suggest any type of electronic transaction processor that "atomically binds" a first element to a second element, and in forming a response transmits a first element "atomically bound" to a second element. However, Challener et al (Col 6, line 65 through Col 7, line 37) specifically teach such binding. Challener et al. discloses a user that authenticates to a system using a PIN number. An authentication server authenticates the PIN number. Once authentication is achieved the Voter ID number is bound to a specific ballot number. This bound association is saved in the data processing records, and a bound ballot is distributed to the voter.

The examiner is considering the term atomically in relation to concurrent programming and operating systems (An atomic operation appears to take effect at some instant during its execution and no other operation observes intermediate states). As

described above, an atomic binding occurs during the process of validating the PIN number, and associating Voter ID number with a specific ballot number.

While in one embodiment the applicant is using a hashed nonce to perform atomic binding, such a technique is not an exclusive method for doing such. A nonce is simply a number used once. This number is often a pseudo-random number that is issued in an authentication protocol to ensure that old communications are not reused (i.e. the voter can only vote once). The use of a nonce is well known in the security community as one of many possible techniques for assisting in authentication. While the Challener et al reference does not explicitly use the term nonce, the examiner notes that on Col 7, lines 15 – 19 that the disclosed system marks the ballot number and voter ID as being "used", thus preventing that particular voter from voting again in this election. Therefore, the voter ID number can only be used once and a nonce has been achieved and is inherently disclosed in Challener et al.

Conclusion

5 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to

37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6 Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Van Bramer whose telephone number is (571) 272-8198. The examiner can normally be reached on 9am - 5pm Monday through Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eric Stamber can be reached on (571) 272-6724. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jvb

ERIC W. STAMBER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600